AMENDMENTS

IN THE CLAIMS:

Please amend claims 1, 4, 10-11 and 15, and add claim 23 as provided below.

1. (Currently Amended): A network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system adapted to be coupled with a host bus in the host system and transfer data between the network interface system and the host system;

a media access control system adapted to be coupled with the network and to transfer data between the network interface system and the network;

a memory system coupled with the bus interface system and the media access control system, the memory system being adapted to store incoming and outgoing data being transferred between the network and the host system;

a security system coupled with the memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data; and

a descriptor management system coupled with the bus interface system and the security system, the descriptor management system being adapted to obtain initialization vector information from the host system and to provide the initialization vector information to the security system;

wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.

2. (Original): The system of claim 1, wherein the security system comprises at least one transmit security processor adapted to selectively encrypt or selectively authenticate the outgoing data.

3. (Original): The system of claim 2, wherein the initialization vector information indicates whether the outgoing data is to undergo cipher block chaining (CBC) encryption in the security system.

4. (Currently Amended): The system of claim 3, wherein the at least one transmit security processor selectively employs an initialization vector (IV) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information from the descriptor management system.

5. (Original): The system of claim 4, wherein the at least one transmit security processor employs the initialization vector (IV) from the outgoing data if the initialization vector information indicates that the outgoing data is to undergo cipher block chaining (CBC) encryption.

6. (Original): The system of claim 4, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

7. (Canceled):

8. (Original): The system of claim 3, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

9. (Original): The system of claim 1, wherein the initialization vector information indicates whether the outgoing data is to undergo cipher block chaining (CBC) encryption in the security system.

10. (Currently Amended): The system of claim 9, wherein the security system selectively employs an initialization vector (IV) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information, and wherein the security system is adapted to use the initial random data string as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.

11. (Currently Amended): The system of claim ~~10~~8, wherein the security system selectively employs the initialization vector (IV) comprising the initial random data string used as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system~~from the outgoing data if the initialization vector information indicates that the outgoing data is to undergo cipher block chaining (CBC) encryption~~.

12. (Original): The system of claim 10, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

13. (Canceled):

14. (Original): The system of claim 1, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

15. (Currently Amended): A method of encrypting outgoing data in a network interface system, the method comprising:

providing initialization vector information from a descriptor to a security system in a network interface system;

selectively encrypting outgoing data according to an initialization vector (IV) comprising an initial random data string from the outgoing data, before security association information has been retrieved by the security system;

selectively encrypting or authenticating outgoing data using the security system; and

selectively employing ~~an~~ the initialization vector (IV) from the outgoing data to perform CBC encryption or authentication of the outgoing data according to the initialization vector information.

16. (Original): The method of claim 15, wherein providing the initialization vector information comprises:

reading a transmit descriptor from a host system; and

providing initialization vector information from the transmit descriptor to the security system.

17. (Original): The method of claim 16, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information whether an initialization vector is present in the outgoing data.

18. (Original): The method of claim 17, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption further comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

19. (Original): The method of claim 16, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises

determining from the initialization vector information a length of an initialization vector in the outgoing data.

20. (Original): The method of claim 15, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information whether an initialization vector is present in the outgoing data.

21. (Original): The method of claim 20, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption further comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

22. (Original): The method of claim 15, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

23. (New): The method of claim 15, further comprising employing the initial random data string as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.